US010298395B1

(12) **United States Patent**
Schiatti et al.

(10) **Patent No.: US 10,298,395 B1**
(45) **Date of Patent: May 21, 2019**

(54) **INTEROPERABILITY OF ZERO-KNOWLEDGE PROOF ENABLED BLOCKCHAINS**

(71) Applicant: **Accenture Global Solutions Limited**, Dublin (IE)

(72) Inventors: **Luca Schiatti**, Juan-les-Pins (FR); **Antoine Rabenandrasana**, Nice (FR); **Hugo Borne-Pons**, Juan-les-Pins (FR); **Giuseppe Giordano**, Juan-les-Pins (FR)

(73) Assignee: **ACCENTURE GLOBAL SOLUTIONS LIMITED**, Dublin (IE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/142,657**

(22) Filed: **Sep. 26, 2018**

(51) **Int. Cl.**
H04L 9/32 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/3221*** (2013.01); ***H04L 9/3239*** (2013.01); *H04L 2209/38* (2013.01)

(58) **Field of Classification Search**
CPC .. H04L 9/3221; H04L 9/3239; H04L 2209/38
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,584,493	B1 *	2/2017	Leavy	H04L 63/104
2018/0117446	A1 *	5/2018	Tran	A61B 5/0022
2018/0315026	A1 *	11/2018	Kraemer	G06Q 20/065

OTHER PUBLICATIONS

Hartwig Mayer, "zk-SNARK explained: Basic Principles," dated Dec. 13, 2016, pp. 1-8, DOI: 10.13140/RG.2.2.20887.68007, published online by ResearchGate at URL https://www.researchgate.net/publication/321124635_zk-SNARK_explained_Basic_Principles.

"Quorum—ZSL Integration: Proof of Concept: Technical Design Document," dated 2017, pp. 1-23, published online by GitHub, Inc. at URL https://github.com/jpmorganchase/zsl-q.

Ariel Gabizon, "How Transactions Between Shielded Addresses Work," Zcash Blog, dated Nov. 29, 2016, pp. 1-5, published online by ZeroCoin Electric Coin Company at URL https://blog.z.cash/zcash-private-transactions/.

(Continued)

Primary Examiner — Meng Li
(74) *Attorney, Agent, or Firm* — Brinks Gilson & Lione

(57) **ABSTRACT**

For shielded cryptographic data exchange interoperation, an interoperability node is in communication with a furnisher participant node of a furnisher distributed ledger technology (DLT) network and a receiver participant node of a receiver DLT network. The interoperability node may obtain a shielded exchange instruction. The shielded exchange instruction may include a zero-knowledge proof, a selected token nullifier, a new token nullifier, and a new token digest. The zero-knowledge proof may be indicative of the furnisher participant having access to the selected token identifier. When the interoperability node determines that the new token nullifier is not present on a receiver blockchain, the interoperability node may submit the shielded exchange instruction to a furnisher smart contract and a receiver smart contract. The furnisher smart contract may retire the selected token nullifier on the furnisher blockchain. The receiver smart contract may insert the new token nullifier and the new token digest to the receiver blockchain.

20 Claims, 7 Drawing Sheets